

Recognizing Work Place Hazards Associated with Microprocessors

R. Dickson and W. McQuiston

December 6, 2000



A Bird in the Hand ...



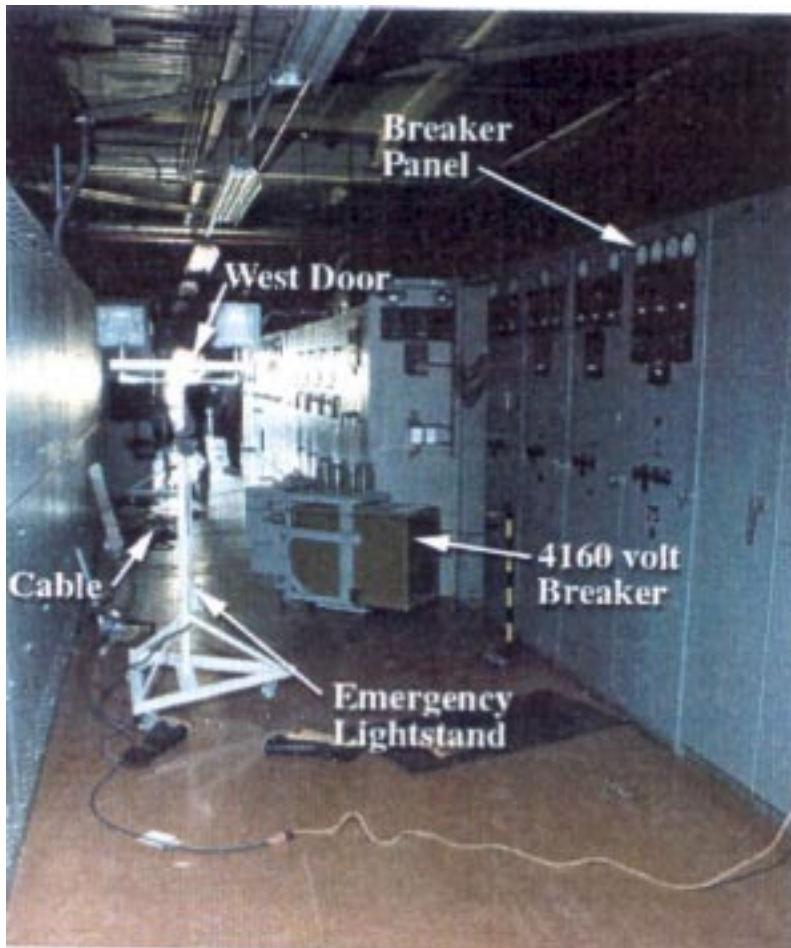
**Awareness & Recognition
that Microprocessors
Introduce an Element of
Complexity to the
Control of Hazards in
the Work Place**



Test Reactor Area

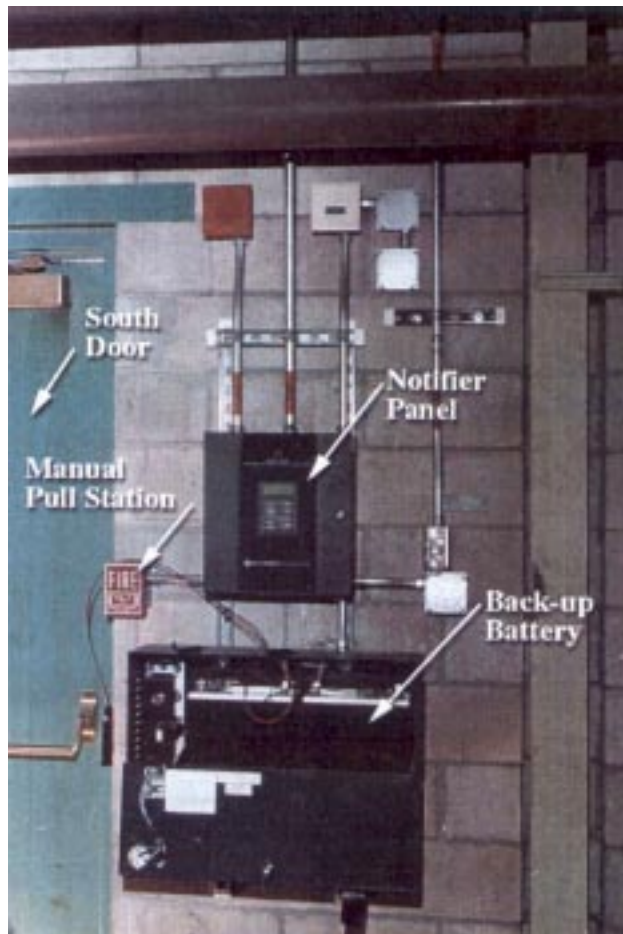
INEEL

Accidental Discharge of CO₂ Fire Suppression System



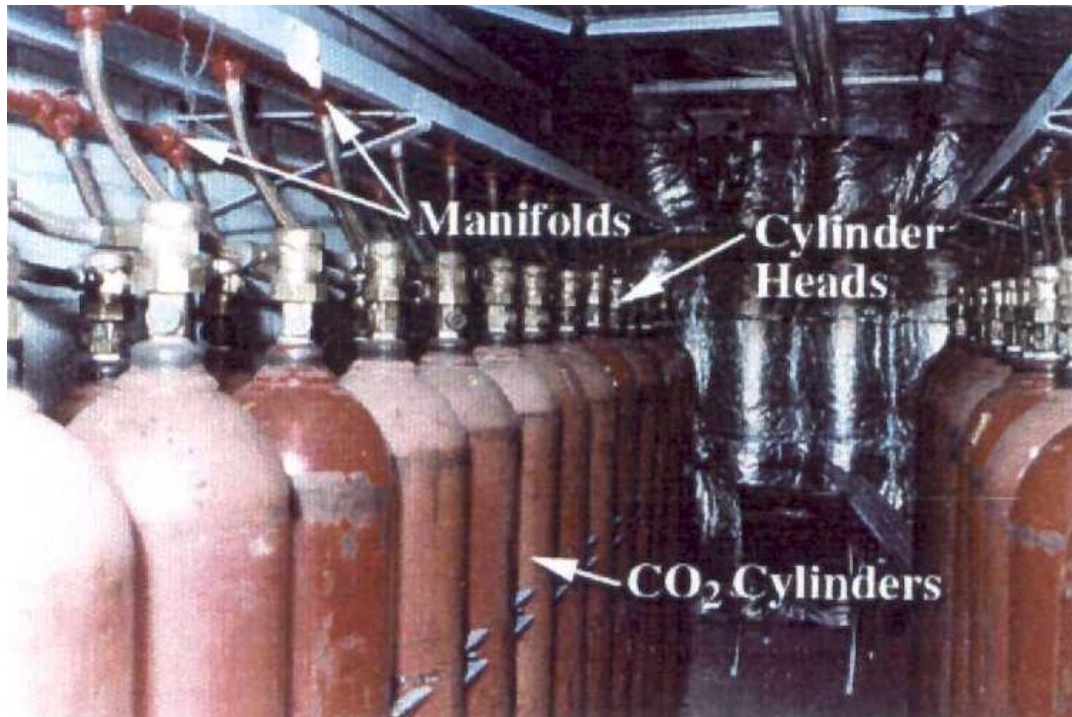
- ***Suppression system installed in 1971 to support reactor operations***
- ***Reactor was inactivated in 1982***
- ***Accident during routine breaker maintenance in July 1998***

Accidental Discharge of CO₂ Fire Suppression System



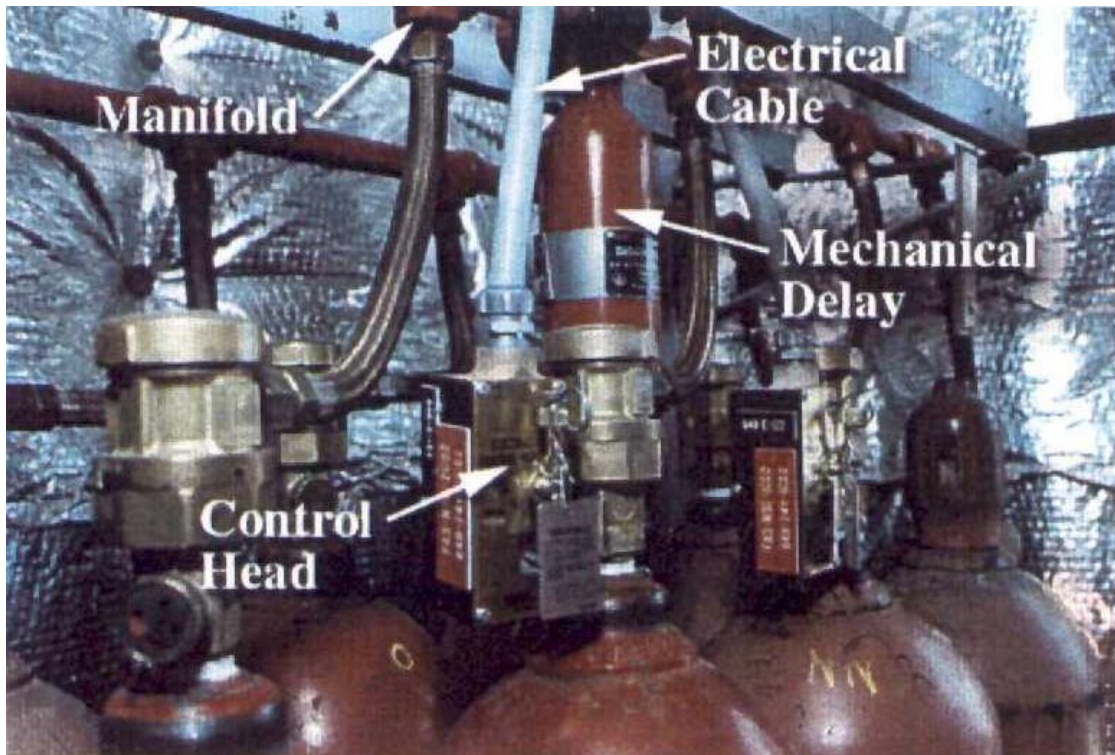
- ***System Modified in 1997 and microprocessor-based alarm panel installed***
- ***Panel had Factory Mutual approval and was listed by Underwriters Laboratory***

Accidental Discharge of CO₂ Fire Suppression System



- ***CO₂ hazard identified in pre-job briefing***
- ***System was “impaired” as a safety barrier and not physically locked out***

Accidental Discharge of CO₂ Fire Suppression System



- ***Spurious signal generated on loss of power activated control heads***
- ***Sensor on mechanical delay not installed (no alarm function)***

Accidental Discharge of CO₂ Fire Suppression System

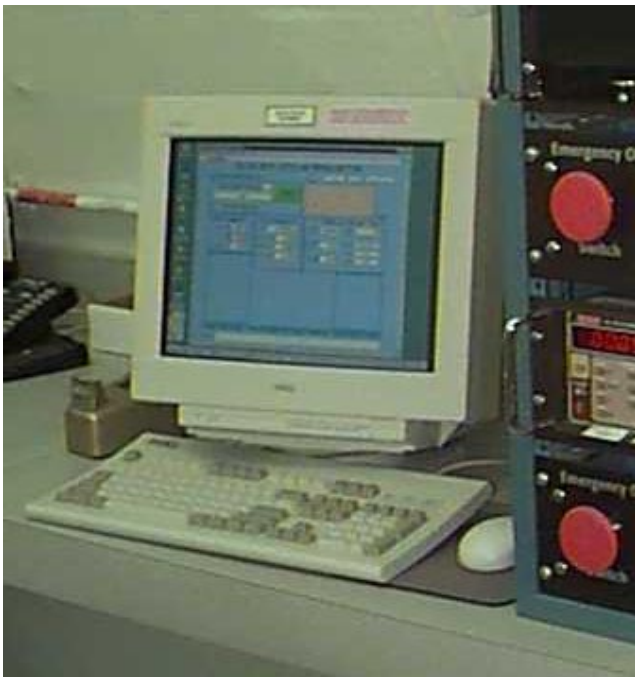
- ***Hazard - CO₂***
- ***Barrier - Electric Control Head***
- ***Computer Controlled the Barrier***
- ***Electronic Impairment versus Lockout***
- ***Sensor not Installed to Detect Barrier Failure***

Inadequate Fail-Safe Capability of Radiation Source Control System



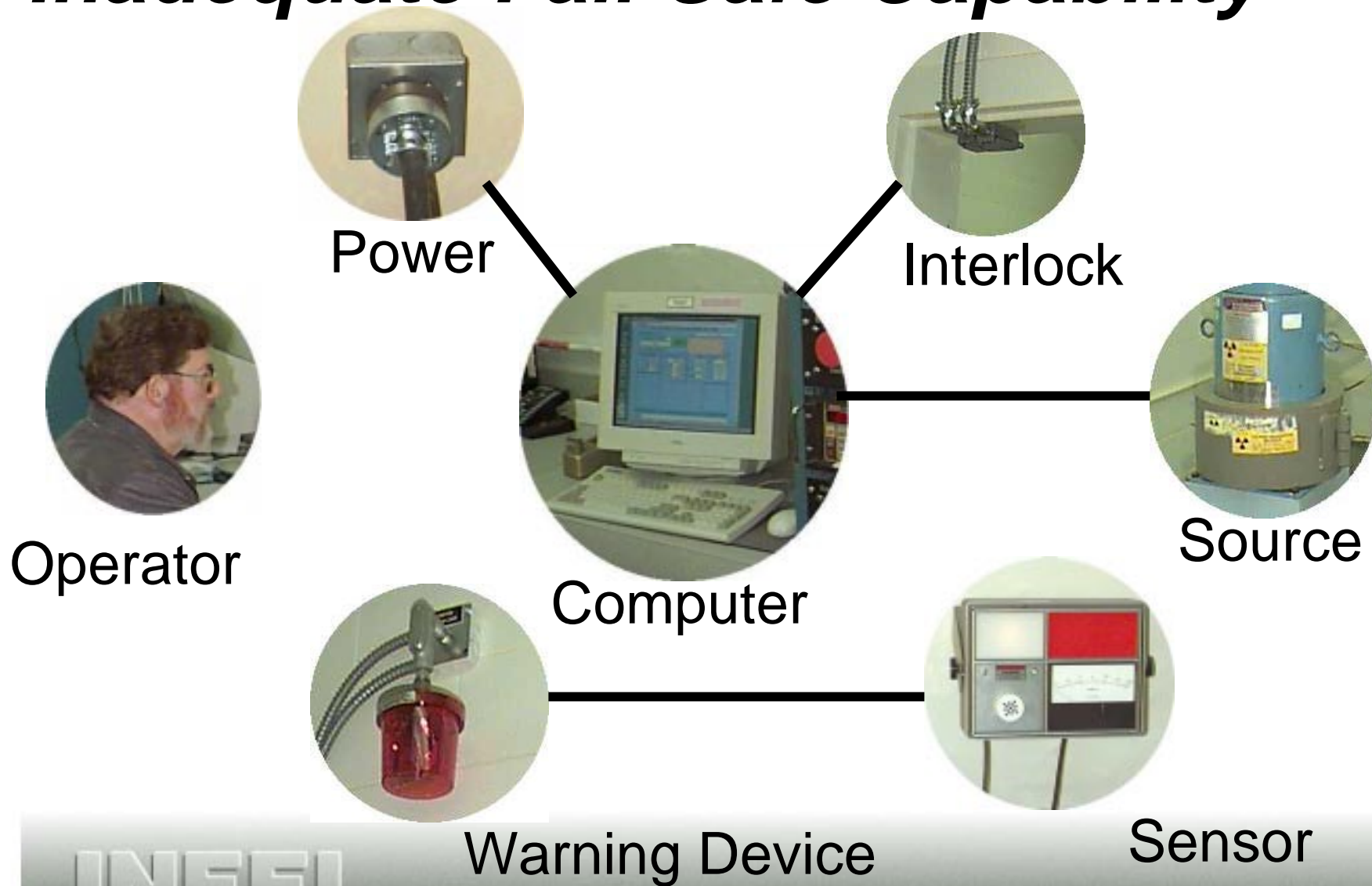
- ***Hazard - Radiation Source***
- ***Barrier - Shielding Wall & Door***
- ***Interlock Switch - Status of Barrier***
- ***Sensor - Radiation Detector***
- ***Warning Alarms - Flashing Light & Audible Signal***

Inadequate Fail-Safe Capability of Radiation Source Control System

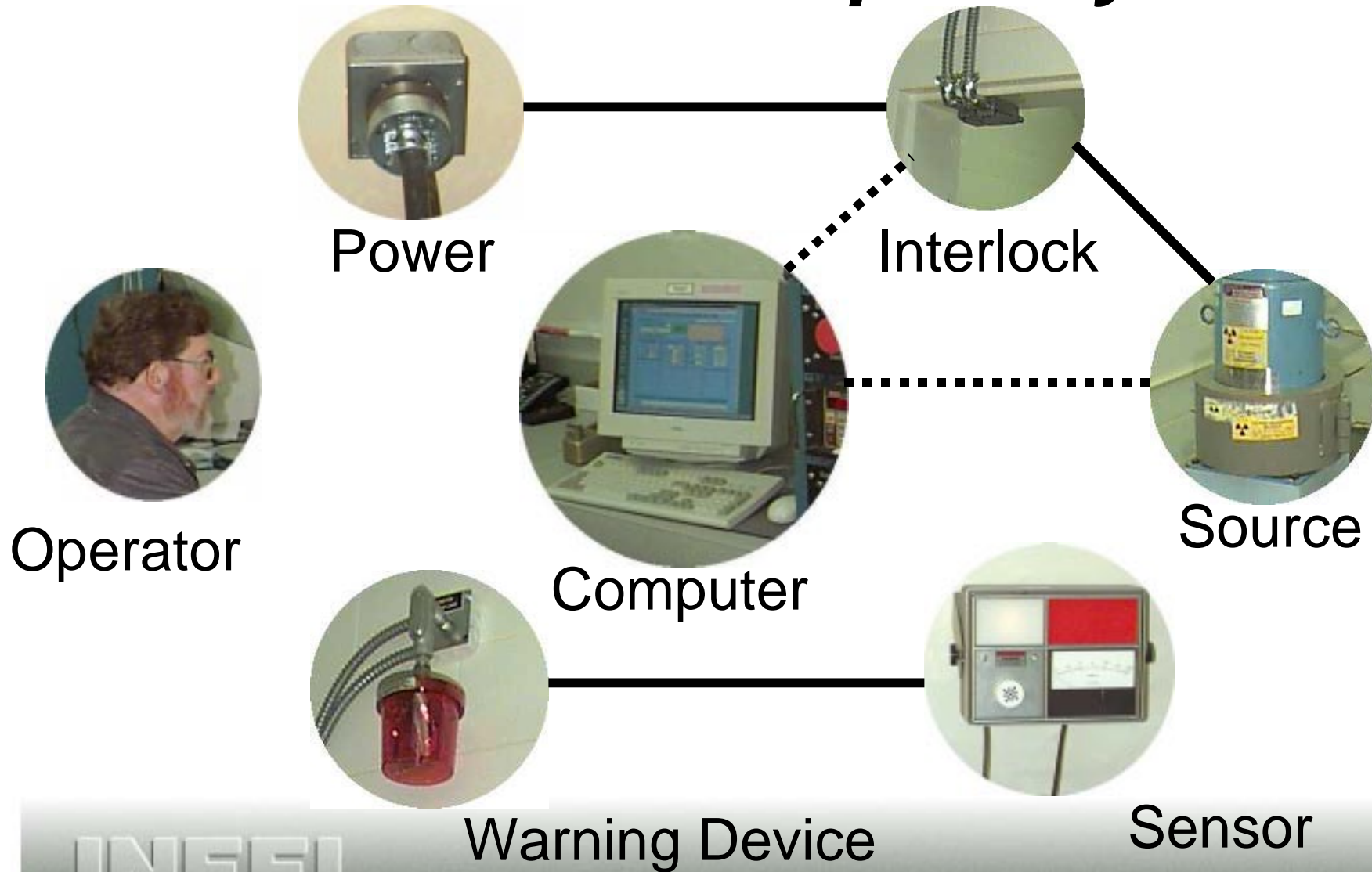


- ***Computer periodically checked status of interlock switch***
- ***Interlock failed when technicians rebooted the computer***
- ***Defense in depth - other design and administrative controls alerted technicians to failure***

Inadequate Fail-Safe Capability



Revised Fail-Safe Capability



Awareness & Recognition



- ***Identify and analyze situations where computers control safety barriers***
- ***Develop and implement controls - plan for defense in depth***